UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/589,747 | 06/09/2000 | Neil Gilbert Siegel | 199.38513X00 | 1612 |

26294 7590 10/21/2004

TAROLLI, SUNDHEIM, COVELL & TUMMINO L.L.P.
526 SUPERIOR AVENUE, SUITE 1111
CLEVEVLAND, OH 44114

| EXAMINER | |
|---|---|
| BACKER, FIRMIN | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 3621 | |

DATE MAILED: 10/21/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 09/589,747 | SIEGEL ET AL. | |
| | Examiner | Art Unit | |
| | Firmin Backer | 3621 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *13 July 2004* .

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-41* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-41* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

**Priority under 35 U.S.C. §§ 119 and 120**

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

**Attachment(s)**

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

***Response to Amendment***

This is in response to an amendment file on July 13th, 2004. In the amendment, claims 1 have been amended, no claim has been canceled, and no claim has been added. Claims 1-41 remain pending in the letter.

***Claim Rejections - 35 USC § 103***

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1-41 are rejected under 35 U.S.C. 103(a) as being unpatentable over Funk (U.S. Patent No. 5,721,779) in view of Keene et al (U.S. PG Pub No. 2004/0049294).

3. As per claim 1, Funk teaches a method of administering access and security on a network having a plurality of computers comprising installing a one-way encrypted password file on each computer of the plurality of computers in the network, wherein the encrypted password file includes a plurality of user identifications, associated encrypted passwords and associated privileges for each authorized user allowed access to the plurality of computers and the network, a password entered by a user when the user logs into a computer of the plurality of computers on the network, checking for a match between the user identification and encrypted password entered by the user and the plurality of user identifications and encrypted passwords stored in the

encrypted password file, enabling access to data and software contained on the computer and the network permitted by the associated privileges for the user when a match is found on the encrypted password file (*see abstract, fig 2, column 4 lines 3-6 line 49)*. Funk fails to teach a filtering and displaying messages to the user permitted by the associated privileges when a match is found on the encrypted password file. However, Keene et al teach filtering and displaying messages to the user permitted by the associated privileges when a match is found on the encrypted password file (*see paragraph 007)*. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the inventive concept of Funk to include Keene et al's filtering and displaying messages to the user permitted by the associated privileges when a match is found on the encrypted password file because this would have provided controlled access to shared objects and documents in a database among approved users by individually defining the scope of their access to the data contained therein thereby displayed to the user as a document file having a redacted document, blocking out the information that the user is not privileged to see.

4. As per claim 2, Funk teaches a method wherein the associated privileges contained in the encrypted password file indicate the security level and access privileges of the user identification for access to software, data and messages contained in the computer, the network, and transmitted over the network (*see abstract, fig 2, column 4 lines 3-6 line 49)*.

5. As per claim 3, Funk teaches a method wherein when one or more attempts of the user entering a user identification and encrypted password have failed to match the plurality of user

identifications and encrypted passwords contained in the encrypted password file, the method further comprising: transmitting to a systems administrator or security officer by the computer a notification of the failure to provide a encrypted user identification and password that matches a user identification and encrypted password stored on the encrypted password file (*see abstract, fig 2, column 4 lines 3-6 line 49).*

6. As per claim 4, Funk teaches a method further comprising locking, upon request by the systems administrator or security officer, the computer being accessed by the user having at least one failed attempt at entering a user identification and encrypted password so as to permit only access to a login screen by the user (*see abstract, fig 2, column 4 lines 3-6 line 49).*

7. As per claim 5, Funk teaches a method further comprising spoofing, upon request by the systems administrator or security officer, the user into believing that the access has been gained to the computer, wherein spoofing includes the presentation of false messages and information to the user (*see column 12 lines 20-64).*

8. As per claim 6, Funk teaches a method further comprising disabling, upon request by the systems administrator or security officer, the computer system so that the user cannot access the computer system (*see column 8 lines 47-63).*

9. As per claim 7, Funk teaches a method further comprising deleting, upon request by the systems administrator or security officer, a plurality of files stored in the computer system (*see abstract, fig 4, column 2 lines 12-46)*.

10. As per claim 8, Funk teaches a method further comprising displaying to a screen on the computer system a request for re-authentication at the direction of a system administrator or a security officer (*see fig 2,3 column 4 lines 30-48)*

11. As per claims 9, Funk teaches a method wherein the request for re-authentication comprises displaying a login screen having a position for entry of the user identification and password (*see abstract, fig 2, column 4 lines 3-6 line 49)*.

12. As per claims 10, Funk teaches a method wherein the user identification is a role or title indicative of a level of authority of the user (*see fig 2,3 column 4 lines 30-48)*.

13. As per claims 11, Funk teaches a method further comprising accessing a master password file on a computer system accessible by the systems administrator or security officer; encrypting the password; and searching the master password file for a match of the user identification and encrypted password (*see abstract, fig 2, column 4 lines 3-6 line 49)*.

14. As per claims 12, Funk teaches a method further comprising disabling the computer system, or spoofing the user, or locking the computer system when a match is not found for the

user identification and encrypted password in the master password file (*see abstract, fig 2, column 4 lines 3-6 line 49)*.

15. As per claims 13, Funk teaches a method wherein after the user has entered the user identification and encrypted password and the user identification and password has matched that found in the encrypted password file, further comprising entering a new password by the user, re-authenticating the user identification and password stored on the master password file, encrypting the new password; and replacing the user identification and password with the encrypted user identification and the new encrypted password in the master password file (*see abstract, fig 2, column 4 lines 3-6 line 49)*

16. As per claims 14, Funk teaches a method further comprising: attaching the master password file to a message, encrypting the message using a private key and passphrase available only to the systems administrator or security officer; and transmitting the message to the plurality of computers (*see fig 4, column 5 lines 38-53, 6 lines 18-50)*.

17. As per claims 15, Funk teaches a method further comprising decrypting the message using a public key corresponding to the private key; reporting to the system administrator or security officer a failure to decrypt the message; and replacing the encrypted password file with the decrypted master password file (*see column 8 lines 47-63)*.

18. As per claims 16, Funk teaches a method further comprising detecting an anomalous event in a computer of the plurality of computers; and reporting the anomalous event to a system administrator or security officer (*see column 12 lines 20-64)*.

19. As per claims 17, Funk teaches a method wherein the anomalous event comprise: the user has exceeded the number of allowable unsuccessful login attempt: a change in the users associated privileges has occurred, a system disable operation was initiated by the user; a user's password has expired, a message was rejected due to an invalid digital signature, a request for remote user re-authentication has been received by the system administrator or security officer, a request for a remote user lockout has been received by the system administrator or security officer; and a request for remote loading passwords has completed successfully on the system administrator or security officer (*see abstract, fig 2, column 4 lines 3-6 line 49)*.

20. As per claims 18, Funk teaches a method further comprising deleting a plurality of files on the computer and disabling the computer in response to an anomalous event when requested by the system administrator or security officer or when an immediate shutdown in requested by the user (*see abstract, fig 2, column 4 lines 3-6 line 49)*.

21. As per claims 19, Funk teaches a method further comprising disabling the computer system, or spoofing the user, or locking the computer system when an anomalous event occurs (*see abstract, fig 2, column 4 lines 3-6 line 49)*.

22. As per claims 20 and 31, Funk teaches a system to administer access and security on a network having plurality of computers comprising includes a one-way encrypted password file on each computer of the plurality of computers in the network, wherein the encrypted password file includes a plurality of user identifications, associated encrypted passwords and associated privileges for each authorized user allowed access to the plurality of computers and the network, a user login module to receive a user identification or role and password from a user and login the user when a match is found in the encrypted password file (*see abstract, fig 2, column 4 lines 3-6 line 49)*. Funk fails to teach a channel monitoring and filtering module to monitor and receive broadcast c multicast messages within the network and display the message to the user when the user's associated privileges permit the viewing of the message. However, Keene et al teach a channel monitoring and filtering module to monitor and receive broadcast c multicast messages within the network and display the message to the user when the user's associated privileges permit the viewing of the message (*see paragraph 007)*. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the inventive concept of Funk to include Keene et al's channel monitoring and filtering module to monitor and receive broadcast c multicast messages within the network and display the message to the user when the user's associated privileges permit the viewing of the message because this would have provided controlled access to shared objects and documents in a database among approved users by individually defining the scope of their access to the data contained therein thereby displayed to the user as a document file having a redacted document, blocking out the information that the user is not privileged to see.

23. As per claims 21 and 32, Funk teaches a system further comprising a password management module to update and insure that all the computers in the network contain the same encrypted password file (*see column 8 lines 47-63)*.

24. As per claims 22 and 33, Funk teaches a system further comprising a remote auditing module to monitor and process anomalous events which may occur on the computer ((*see abstract, fig 2, column 4 lines 3-6 line 49)*.

25. As per claims 23 and 34, Funk teaches a system wherein the anomalous events comprise: the user has exceeded the number of allowable unsuccessful login attempts; a change in the users associated privileges has occurred, a system disable operation was initiated by the user; a user's password has expired, a message was rejected due to an invalid digital signature, a request for remote user re-authentication has been received by the systems administrator or security officer, a request for a remote user lockout has been received by the system administrator or security officer; and a request for remote loading passwords has completed successfully on the system administrator or security officer (*see column 9 lines 8-63)*.

26. As per claims 24 and 35, Funk teaches a system further comprises a remote control module to enable a systems administrator or security officer to take appropriate action when an event transpires, wherein the event is an anomalous event (*see column 8 lines 47-63)*.

27. As per claims 25 and 36, Funk teaches a system wherein the appropriate action comprises disabling, upon request by the systems administrator or security officer, the computer system so that the user cannot access the computer system; and deleting, upon request by a systems administrator or security officer, a plurality of files stored in the computer (*see abstract, fig 2, column 4 lines 3-6 line 49).*

28. As per claims 26 and 37, Funk teaches a system wherein the appropriate action comprises spoofing, upon request by a systems administrator or security officer, the user into believing that the access has been gained to the computer, wherein spoofing includes the presentation of false messages and information to the user (*see abstract, fig 2, column 4 lines 3-6 line 49).*

29. As per claims 27 and 38, Funk teaches a system wherein the appropriate action comprises: locking the computer, upon request of a systems administrator or security officer, and displaying a login screen for the user to re-authenticate the user identification and password (*see abstract, fig 2, column 4 lines 3-6 line 49).*

30. As per claims 28 and 39, Funk teaches a system further comprising an authentication module to re-authenticate the user after the user login module has found a match in the encrypted password contained in the computer by checking the user identification and password against a master password file stored in a computer accessible by a systems administrator or security officer (*see abstract, fig 2, column 4 lines 3-6 line 49).*

31. As per claims 29 and 40, Funk teaches a system wherein the password management module attaches a master password file containing a complete user identifications, associated encrypted passwords and associated privileges to a message, encrypts the message using a private key and pass phrase for the system administrator or security officer and broadcasts the message to all users (*see abstract, fig 2, column 4 lines 3-6 line 49)*.

32. As per claims 30 and 41, Funk teaches a system wherein the password management module decrypts the message using a public key associated with the private key, replaces the encrypted password file when decryption of the message is successful and reports a failure to the system administrator or security officer when the decryption is not successful (*see abstract, fig 2, column 4 lines 3-6 line 49)*.

***Response to Arguments***

33. Applicant's arguments filed July 13th, 2004 have been fully considered but they are not persuasive.

a. Applicant argue that the prior art fail to teach filtering and display of broadcast or multicast messages based upon user privileges. Applicant further define multicast message to have at least to intended destinations and argues that neither art taken alone or in combination teach filtering of multicast message as recite in claims 1, 20 and 31. Examiner respectfully disagrees with Applicant characterization of the prior art. Keene

taken alone teaches that after given an access identification, a user can access the database system and request access to an object. The system then retrieves information pertaining to the individual user's privilege criteria and determines which information contained in the database may be accessed by the requestor. The system then filters the information including objects, their attributes and associated documents according to the privilege information and gives the user limited access to the information. The requested and approved information can then be sent to the requestor of the information. This message/information could also be displayed to the user as a document file having a redacted document, blocking out the information that the user is not privileged to see. Keene further teach that access to objects and associated documents can also be limited to read-only privileges. It can be limited even further to read-only privileges to particular objects, their attributes, associated documents and other information. Privileges could be limited to viewing the object itself, to viewing only certain attributes of an object and to view only certain attached documents. Privileges could also be expanded to modification privileges. With modification privileges, a user can modify the data to which it has access by either adding or deleting information and attaching or removing other documents associated with the objects. This enables a type of data exchange between the host and other privileged users (*see paragraphs 7 and 8)*. Applicant accentuates more on multicast message. The amended claim recite ***broadcast or multicast message***. This is to indicate either or is sufficient to make the system operational.

b. Applicant further argues that Funk does not discuss transmitting notification of fail attempts to a system operator. Examiner respectfully disagrees with applicant characterization Funk's inventive concept. Funk teach that the encrypted value generated can be provided as a challenge signal through a communication port to a party requesting access through a security system. This step provides a challenge signal to a client that can be operated on by a one-way commutative function to generate a response signal that represents the challenge signal encrypted with an offered password signal. As further the response signal can be transmitted by the client to the system operator and collected by the system for comparison with the authentication values stored in the database memory.

c. Applicant further argues that neither of the prior art teaches providing an unauthencicated user with false data. Funk teach modifications of the system that can include randomizing a password signal selected by a user, or for digesting the response signal and the key signal being compared. Other modifications can include generating separate base signals or prime number signals for each authentication value, or for a series of authentication values.

***Conclusion***

**THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO

MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Firmin Backer whose telephone number is (703) 305-0624. The examiner can normally be reached on Mon-Thu 9:00 AM - 5:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James Trammell can be reached on (703) 305-9768. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Firmin Backer
Primary Examiner
Art Unit 3621

October 17, 2004